KEIO SCIENCE AND TECHNOLOGY REPORTS
VOL. 44, NO. 1, pp. 1-6, 1991, ISSN: 02864215

ON THE GALOIS GROUP OF $x^n - x^{n-1} - x^{n-2} - \cdots - x - 1 = 0$

by

Kenzo Komatsu

Department of Mathematics
Faculty of Science and Technology, Keio University
Hiyoshi, Yokohama 223, Japan

(Received November 5, 1991)

1. In his doctoral thesis [4], Tamura obtained an interesting result on the irreducibility of certain polynomials: *Let $k_1, k_2, \cdots, k_{n-1} (n>1)$ be rational integers such that*

$$k_{n-1} \geq k_{n-2} \geq \cdots \geq k_2 \geq k_1 \geq 1 \ .$$

Then the polynomial

$$F(x) = x^n - k_{n-1}x^{n-1} - k_{n-2}x^{n-2} - \cdots - k_1 x - 1$$

is irreducible over the rational number field $\boldsymbol{Q}$. See [5], Lemma 10.

Consider now the following question: Is it possible to determine the Galois group of $F(x)=0$ over $\boldsymbol{Q}$? It seems very difficult to solve this problem completely. However, for the simplest case

$$k_1 = k_2 = \cdots = k_{n-1} = 1 \ ,$$

we obtain

Theorem 1. *The Galois group of the equation*

$$x^n - x^{n-1} - x^{n-2} - \cdots - x - 1 = 0$$

over $\boldsymbol{Q}$ is the symmetric group S_n for every $n>1$.

The purpose of this paper is to prove Theorem 1. We require a few theorems from algebraic number theory, including Minkowski's inequality on the discriminant of an algebraic number field.

2. Let α be a root of

(2.1) $$f(x) = x^n - x^{n-1} - \cdots - x - 1 = 0 \ .$$

Since

(2.2) $$(x-1)f(x) = x^{n+1} - 2x^n + 1 \ ,$$

we have

$$\alpha^{n+1}-2\alpha^{n}+1=0\ . \tag{2.3}$$

Also, by (2.2),

$$(\alpha-1)f'(\alpha)=(n+1)\alpha^{n}-2n\alpha^{n-1}\ .$$

Hence

$$(1-\alpha)f'(\alpha)=\alpha^{n-1}\{2n-(n+1)\alpha\}\ . \tag{2.4}$$

3. For any $\xi\in\boldsymbol{Q}(\alpha)$, we denote by $N(\xi)$ its norm in $\boldsymbol{Q}(\alpha)$. For any $a\in\boldsymbol{Q}$, we have

$$N(a-\alpha)=f(a)\ . \tag{3.1}$$

Hence

$$N(1-\alpha)=f(1)=1-n\ . \tag{3.2}$$

Also, for any a, $b\in\boldsymbol{Q}(b\neq0)$, we have

$$N(a-b\alpha)=b^{n}N\left(\frac{a}{b}-\alpha\right)=b^{n}f\left(\frac{a}{b}\right)\ . \tag{3.3}$$

Hence

$$N(2n-(n+1)\alpha)=(n+1)^{n}f\left(\frac{2n}{n+1}\right)\ .$$

Now, by (2.2),

$$\left(\frac{2n}{n+1}-1\right)f\left(\frac{2n}{n+1}\right)=\left(\frac{2n}{n+1}\right)^{n+1}-2\left(\frac{2n}{n+1}\right)^{n}+1\ ,$$

$$\frac{n-1}{n+1}f\left(\frac{2n}{n+1}\right)=\left(\frac{1}{n+1}\right)^{n+1}((n+1)^{n+1}-2(2n)^{n})\ .$$

Hence

$$N(2n-(n+1)\alpha)=\frac{(n+1)^{n+1}-2(2n)^{n}}{n-1}\ . \tag{3.4}$$

Now let

$$\delta=f'(\alpha)\ ,\quad D=N(\delta)\ . \tag{3.5}$$

Then, from (2.4), (3.2) and (3.4), we obtain

$$\begin{aligned}(1-n)D&=N(\alpha^{n-1})\frac{(n+1)^{n+1}-2(2n)^{n}}{n-1}\\&=(-1)^{n-1}\frac{(n+1)^{n+1}-2(2n)^{n}}{n-1}\ ,\end{aligned}$$

since

(3.6) $$N(\alpha^{n-1})=(N(\alpha))^{n-1}=((-1)^{n+1})^{n-1}=(-1)^{n-1}\ .$$

Hence

(3.7) $$D=(-1)^{n-1}\frac{2(2n)^n-(n+1)^{n+1}}{(n-1)^2}\ .$$

4. Define the ring M by

$$\begin{aligned}M&=[1,\alpha,\cdots,\alpha^{n-1}]\\&=\{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}|a_i\in\boldsymbol{Z}\}\ .\end{aligned}$$

Let $\alpha_0=\alpha-1$. Then, by (2.3),

$$(\alpha_0+1)^{n+1}-2(\alpha_0+1)^n+1=0\ .$$

Hence

$$\alpha_0^{n+1}+b_n\alpha_0^n+\cdots+b_2\alpha_0^2+(1-n)\alpha_0=0\ ,$$

where $b_i\in\boldsymbol{Z}$. Hence

$$\frac{n-1}{\alpha_0}=\alpha_0^{n-1}+b_n\alpha_0^{n-2}+\cdots+b_2\in M\ .$$

By (3.2) we see that

(4.1) $$\frac{N(1-\alpha)}{1-\alpha}\in M\ .$$

Let $a\in\boldsymbol{Q}$, $a\neq1$, and let $\beta=\alpha-a$. Then, by (2.3),

$$(\beta+a)^{n+1}-2(\beta+a)^n+1=0\ ,$$

and so

$$\beta^{n+1}+\{(n+1)a-2\}\beta^n+\cdots+(a^{n+1}-2a^n+1)=0\ .$$

On the other hand, by (2.2),

$$a^{n+1}-2a^n+1=(a-1)f(a)\ .$$

Hence

$$\beta^n+\{(n+1)a-2)\beta^{n-1}+\cdots+\frac{(a-1)f(a)}{\beta}=0\ .$$

Now

$$\begin{aligned}\beta^n&=(\alpha-a)^n=\alpha^n-na\alpha^{n-1}+\cdots+(-1)^na^n\\&=(\alpha^{n-1}+\cdots+1)-na\alpha^{n-1}+\cdots+(-1)^na^n\\&=(1-na)\alpha^{n-1}+\cdots+\{(-1)^na^n+1\}\ ,\end{aligned}$$

$$\{(n+1)a-2\}\beta^{n-1}=\{(n+1)a-2\}(\alpha^{n-1}-\cdots+(-a)^{n-1})\ .$$

Hence

$$\frac{N(a-\alpha)}{a-\alpha}=\alpha^{n-1}+t_{n-2}\alpha^{n-2}+\cdots+t_1\alpha+t_0\ , \tag{4.2}$$

where $t_i \in \boldsymbol{Q}$. Now let $a, b \in \boldsymbol{Q}$, $a \neq b$, $b \neq 0$. Then

$$\frac{N(a-b\alpha)}{a-b\alpha}=b^{n-1}\cdot\frac{N\left(\frac{a}{b}-\alpha\right)}{\frac{a}{b}-\alpha}=b^{n-1}\alpha^{n-1}+s_{n-2}\alpha^{n-2}+\cdots+s_1\alpha+s_0\ , \tag{4.3}$$

where $s_i \in \boldsymbol{Q}$. From this we obtain

$$\frac{N(2n-(n+1)\alpha)}{2n-(n+1)\alpha}=(n+1)^{n-1}\alpha^{n-1}+c_{n-2}\alpha^{n-2}+\cdots+c_1\alpha+c_0\ , \tag{4.4}$$

where $c_i \in \boldsymbol{Q}$.

5. By Theorem 1 of [2] we see that $D/\delta \in M$. Let

$$D/\delta=x_0+x_1\alpha+\cdots+x_{n-1}\alpha^{n-1}\ , \quad x_i \in Z\ . \tag{5.1}$$

Let p denote a prime number such that

$$p|x_0,\ p|x_1,\ \cdots,\ p|x_{n-1}\ . \tag{5.2}$$

Then

$$\frac{D}{p\delta} \in M\ . \tag{5.3}$$

From (2.4) and (3.5) we obtain

$$\frac{N(1-\alpha)}{1-\alpha}\cdot\frac{D}{\delta}=\frac{N(\alpha^{n-1})}{\alpha^{n-1}}\cdot\frac{N(2n-(n+1)\alpha)}{2n-(n+1)\alpha}\ .$$

Hence, by (3.6),

$$\frac{N(2n-(n+1)\alpha)}{p(2n-(n+1)\alpha)}=(-1)^{n-1}\alpha^{n-1}\cdot\frac{N(1-\alpha)}{1-\alpha}\cdot\frac{D}{p\delta}\ .$$

Since M is a ring, it follows from (4.1) and (5.3) that

$$\frac{N(2n-(n+1)\alpha)}{p(2n-(n+1)\alpha)} \in M\ . \tag{5.4}$$

Since $1, \alpha, \cdots, \alpha^{n-1}$ are linearly independent over Q, by (4.4) and (5.4) we see that $n+1$ is divisible by p. On the other hand D is divisible by p ((5.1) and (5.2)). Hence, by (3.7), $p=2$. From Theorem 1 of [2] we obtain:

(5.5) *For every odd prime p, the discriminant d of $\boldsymbol{Q}(\alpha)$ is not divisible by p^2.*

6. Suppose that n is even. Then, by (3.7), D is odd. Since $d|D$, it follows from (5.5) that d is square-free. Hence the Galois group of $f(x)=0$ is the symmetric group S_n ([3], Theorem 1).

7. Suppose that n is odd. We require two lemmas.

Lemma 1. *Let d_K denote the discriminant of an algebraic number field K of degree $n>1$. Then $|d_K|>2^{n-1}$.*

Proof. From Minkowski's inequality ([1], § 18) and Stirling's formula, we obtain

$$\begin{aligned}|d_K|&>\left(\frac{\pi}{4}\right)^n\left(\frac{n^n}{n!}\right)^2\\&>\left(\frac{\pi e^2}{4}\right)^n\frac{e^{-1/6n}}{2\pi n}.\end{aligned}$$

It is easily seen that

$$\begin{aligned}\log\left\{\left(\frac{\pi e^2}{4}\right)^n\frac{e^{-1/6n}}{2\pi n}\right\}&=n(\log\pi+2-2\log 2)-\frac{1}{6n}-\log(2\pi n)\\&>(n-1)\log 2=\log 2^{n-1}.\end{aligned}$$

Hence we obtain

$$|d_K|>2^{n-1}.$$

Lemma 2. *For any odd integer $n>1$,*

$$D_n=\frac{2(2n)^n-(n+1)^{n+1}}{(n-1)^2}$$

is exactly divisible by 2^{n-1}.

Proof. Let $n=2m+1$, $m\in\boldsymbol{Z}$, $m\geq 1$. Then

$$(2m)^2D_n=2^{n+1}(2m+1)^n-2^{n+1}(m+1)^{n+1},$$

and so

$$m^2D_n=2^{n-1}\{(2m+1)^n-(m+1)^{n+1}\}. \tag{7.1}$$

If m is odd, then both m^2 and $(2m+1)^n-(m+1)^{n+1}$ are odd, and D_n is exactly divisible by 2^{n-1}. Suppose that m is even. Now, by (7.1),

$$\begin{aligned}m^2D_n&=2^{n-1}\left\{\sum_{k=0}^{n-2}{}_nC_k(2m)^{n-k}+n(2m)+1-\sum_{k=0}^{n-1}{}_{n+1}C_km^{n+1-k}-(n+1)m-1\right\}\\&=2^{n-1}m^2\left(\sum_{k=0}^{n-2}{}_nC_k2^{n-k}m^{n-2-k}-\sum_{k=0}^{n-1}{}_{n+1}C_km^{n-1-k}+2\right).\end{aligned}$$

Hence D_n is divisible by 2^{n-1}. Since m is even,

$$\frac{D_n}{2^{n-1}} \equiv {}_{n+1}C_{n-1} = \frac{n(n+1)}{2}$$
$$= n(m+1) \equiv 1 \pmod 2 .$$

Hence D_n is exactly divisible by 2^{n-1}.

Now we prove our theorem for odd $n(n>1)$. It follows from Lemma 2 that D is exactly divisible by 2^{n-1}. Since D is divisible by the discriminant d of $\boldsymbol{Q}(\alpha)$, it follows from (5.5) that

(7.2) $$|d| = 2^t b , \quad t \leq n-1 ,$$

where b is a square-free odd integer. Lemma 1 implies that $b>1$; the discriminant d is exactly divisible by a prime number q. Hence the Galois group G of $f(x)=0$ over $\boldsymbol{Q}$, which is a transitive permutation group on the set $\{1, 2, \cdots, n\}$, contains a transposition ([6]). Suppose that $\boldsymbol{Q}(\alpha)$ has a subfield F such that

$$\boldsymbol{Q} \subset F \subset \boldsymbol{Q}(\alpha) , \quad F \neq \boldsymbol{Q} , \quad F \neq \boldsymbol{Q}(\alpha) .$$

Let d_F denote the discriminant of F, and let

$$m = [\boldsymbol{Q}(\alpha) : F] , \quad k = [F : \boldsymbol{Q}] .$$

Then d is divisible by d_F^m ([1], Satz 39). Since $m>1$, it follows from (7.2) that $|d_F|$ is a power of 2:

$$|d_F| = 2^s .$$

Since $k>1$, it follows from Lemma 1 that $s \geq k$. Hence d_F is divisible by 2^k, and d is divisible by $2^{km}=2^n$. However, it follows from (7.2) that d is not divisible by 2^n. A contradiction proves that G is primitive ([7], Theorem 7.4). Hence we obtain $G=S_n$ ([7], Theorem 13.3).

References

[1] D. Hilbert, Die Theorie der algebraischen Zahlkörper, Jahresber. Deutsch. Math.-Verein., **4** (1897), 175–546.

[2] K. Komatsu, Integral bases in algebraic number fields, J. Reine Angew. Math., **278/279** (1975), 137–144.

[3] K. Komatsu, Square-free discriminants and affect-free equations, Tokyo J. Math., **14** (1991), 57–60.

[4] J. Tamura, A class of transcendental numbers with explicit g-adic expansion and Jacobi-Perron algorithm, Keio University, 1990.

[5] J. Tamura, A class of transcendental numbers having explicit g-adic and Jacobi-Perron expansions of arbitrary dimension, to appear.

[6] B. L. van der Waerden, Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen, Math. Ann., **111** (1935), 731–733.

[7] H. Wielandt, Finite permutation groups, Academic Press, 1964.